

BUSINESS INSIDER UK

Tesla's Amazon cloud account was hacked and used to mine cryptocurrency



MARK MATOUSEK
FEB. 20, 2018, 4:42 PM



Tesla paid RedLock over \$3,000 for discovering the hack as part of its bug bounty program.

OnInnovation / Flickr

- **Tesla's Amazon Web Services account was hacked to mine cryptocurrency.**
- **The hack, which was first brought to Tesla's attention by the cybersecurity startup RedLock, also exposed some of Tesla's proprietary data related to mapping, telemetry, and vehicle servicing.**
- **Tesla said it believes the hack was limited to the company's test cars and did not affect any vehicles owned by its customers.**

Tesla's Amazon Web Services account was hacked to mine cryptocurrency, [Fortune first reported](#). The hack, which was brought to Tesla's attention by the cybersecurity startup RedLock, also reportedly exposed some of Tesla's proprietary data related to mapping, telemetry, and vehicle servicing.

RedLock discovered the hack after it found an IT administrative console that didn't have a password, but the company was unable to determine who initiated the hack or how much cryptocurrency was mined. According to Fortune, Tesla paid RedLock over \$3,000 as part of its [bug bounty program](#), which rewards people who find vulnerabilities in the company's products or services that could be exploited by hackers.

"We maintain a bug bounty program to encourage this type of research, and we addressed this vulnerability within hours of learning about it," a Tesla spokesperson told Business Insider in an email. "The impact seems to be limited to internally-used engineering test cars only, and our initial investigation found no indication that customer privacy or vehicle safety or security was compromised in any way."

Amazon Web Services (AWS) is the retailer's cloud storage division, and it has become one of the company's [most profitable services](#). But AWS accounts, along with business and government websites and servers, have become vulnerable to "[cryptojacking](#)" schemes in which hackers [break into them](#) to mine cryptocurrency, which has become increasingly lucrative in the past year.

"Given the immaturity of cloud security programs today, we anticipate this type of cybercrime to increase in scale and velocity," RedLock CTO Gaurav Kumar said in a statement to Business Insider.

The hack also demonstrated one of the primary concerns auto companies face as they race to introduce the first autonomous vehicles and ride-sharing services. Having proprietary data or technology exposed to competitors could be the difference between being one of the first entrants into the self-driving car market and playing catch-up.

That difference could end up costing companies billions of dollars, which is why Waymo [sued Uber](#) after alleging that Anthony Levandowski, a former Uber engineer who joined the company after working at Waymo, stole confidential information from Waymo that was used by Uber to develop lidar sensors for self-driving vehicles. Uber gave Waymo [\\$245 million in equity](#) as part of a settlement.



EXCLUSIVE FREE REPORT:

The Bitcoin 101 Report by the BI Intelligence Research Team.

[Get the Report Now »](#)

